Abstract

A random number generation device comprises a pseudo random number generation section that is capable of outputting random numbers of a plurality of different pseudo random number sequences, a physical random number generation section for generating physical random numbers, and a switching section for switching the pseudo random number sequence of random numbers output by the pseudo random number generation section on the basis of the physical random numbers generated by the physical random number generation section, where the output of the pseudo random number generation section is used as output random numbers. Since the plurality of different pseudo random number sequences are switched and output according to the physical random numbers, predictability of the random numbers can be reduced in comparison to a conventional random number generation device that uses only pseudo random numbers. Furthermore, since the physical random numbers are not directly used as the output random numbers, any adverse effect on the predictability of the output random numbers is substantially reduced compared with a conventional device even if the physical random number generating means are somehow manipulated from the outside.